

A SYSTEM FOR REALTIME CONFIGURATION OF SUBSCRIBER IDENTITY MODULE (SIM) CARD

FIELD OF INVENTION

5

The present invention relates to SIM card management system. More particularly, it relates to a system for remote configuration and/or re-configuration of a subscriber identity module by means of Over-the-Air (OTA) technology.

10 BACKGROUND

Mobile device advertising through SMS has been widely adapted and it has been coming more popular with the increasing growth of mobile phone users. SMS marketing uses real time mobile traffic to broadcast the marketing messages. Once the marketing message is received, it stays at the SMS inbox until the users delete it.

15 Mobile phone users who received the marketing message may choose whether to read them. It is possible that the mobile phone users may ignore the marketing message if they are not interested at all.

As mentioned, SMS marketing messages use real time mobile traffic to broadcast to users. When a mobile phone operator has to broadcast a message at a
20 specific time, such as a New Year's greeting message to all of its subscribers at 00:00hr at 1 January, it may not even be possible as there may not be sufficient

bandwidth to handle such a huge amount of traffic considering that the subscribers are also sending greeting messages at the same time.

Subscriber Identity Module (SIM) cards store the international mobile
5 subscriber identity (IMSI) and related security information. The information may include the SIM card's unique serial number (ICCID), international mobile subscriber identity (IMSI), security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to and passwords (such as a personal identification number (PIN) and a personal
10 unblocking code (PUK)). These information are pre-coded on the SIM cards.

Updating text messages stored on SIM cards, especially which have been installed and activated on a communication devices, have been a tedious and cost-inefficient task. Any updates and reconfigurations on these SIM cards have to be
15 carried out; generally by having these SIM cards in the field returned from the subscribers, typically to the service provider or network operator. Otherwise, the subscribers may have to purchase a new SIM card from the respective network operators to replace the current SIM card. This eventually causes undue inconvenience to the subscribers, in most cases.

In view of above, it is therefore exist a need for an efficient and yet cost-effective system for remote configuring or re-configuring pre-loaded SIM Card messages/texts of a SIM card residing on a communication device.

5 SUMMARY

In one aspect, the present invention discloses a system for remote configuring or re-configuring pre-loaded SIM Card messages/texts of a SIM card residing on a communication device. This remote configuration system includes a locally situated
10 back-end host server connected to at least one carrier's network, wherein the carrier's network communicates the back-end host server with at least one SIM Card that is associated with the carrier's network; and an Over-The-Air (OTA) gateway adapted to direct management commands received from the back-end host server to its actual recipient SIM card.

15

BRIEF DESCRIPTION OF THE DRAWING

Other objects, features, and advantages of the invention will be apparent from the following description when read with reference to the accompanying drawings. In
20 the drawings, wherein like reference numerals denote corresponding parts throughout the several views:

FIG. 1 illustrates overall system architecture of a remote SIM card configuration system according to one embodiment of the present invention;

FIG. 2 exemplifies a screen shot from a mobile device as one embodiment;

5

FIG. 3 exemplifies a screen shot of the graphical user interface (GUI) of another embodiment;

FIG. 4 exemplifies another screen shot on a mobile device in another
10 embodiment.

DETAILED DESCRIPTION

Embodiments of the present invention shall now be described in detail, with reference to the attached drawings. It is to be understood that no limitation of the
15 scope of the invention is thereby intended, such alterations and further modifications in the illustrated device, and such further applications of the principles of the invention as illustrated therein being contemplated as would normally occur to one skilled in the art to which the invention relates.

20 The present invention provides a system and method for enabling pre-loaded SIM Card Messages/Texts to be configurable and updatable at a desired timing through a secure remote host server and text input interface. The desire timing can be

in timed intervals, pre-set times or ad-hoc times. The configurations can be done in real-time via OTA by a remote entity who is in direct or indirect collaboration with a telecommunications carrier. The SIM cards can be re-configured remotely by sending a secure SMS to the communication devices where the SIM cards are resided.

5

FIG. 1 illustrates schematically a SIM card configuration system 10 in accordance with one embodiment of the present invention. The system 10 provide means for remotely configuring or re-configuring pre-loaded SIM Card messages/texts of a SIM card residing on a communication device 300, from a remote location. Under the system 10, test messages that are pre-loaded on a SIM Card can be independently configured and/or re-configured, via a securely managed user interface device provided at the remote host server. Configuration and/or reconfiguration of the SIM Cards can be carried out on timed-interval, pre-set times, and ad-hoc times basis. Further, the portability and interoperability with multiple mobile devices allows the provision of network specific services and customizations irrespective of end-user device and that can increase operator value to the subscribers and encourage greater loyalty.

The SIM card configuration system 10 comprises mobile devices 300, a SIM message administration back-end host server 100, and an Over-The-Air (OTA) gateway (200). Each mobile device 300 is installed with an activated SIM card that is preloaded with default text string. The back-end host server 100 is securely

20

connected to at least one carrier's network having their own OTA gateway 200. The mobile devices 300 are operationally connected to the respective carrier over a silent SMS channel 400. Specifically, the mobile devices 400 are configured to receive secured message encrypted by a Remote File Management (RFM) via the silent SMS channel 400. The RFM is an enhancement of the OTA gateway 200. It facilitates for content management (e.g. remove, add, update etc.) on the SIM card under a standardized and secured way.

In another embodiment, it is possible that the OTA gateway 200 is an aggregated OTA operated by a third party provider.

The back-end host server 100 includes at least one user interface module and a SIM card database. The SIM card database is a storage where identification details of each SIM card are stored. The identification details include the International Mobile Subscriber Identity (IMSI), the Mobile Subscriber Integrated Services Digital Network Number (MSISDN), the manufacturer vendor, and the serial number of the SIM card. The SIM card further comprises default messages that are stored on an immutable memory space by the card manufactures using standard STK format notations.

The user interface module adapted for allowing administrators to generate and forward configurations and/or re-configurations to mobile devices 300. The

configurations and/or re-configurations are in the form of encrypted RFM messages. The encrypted RFM messages are readily retrievable and readable by the SIM card residing on the mobile devices 300. Suitably, the encrypted RFM messages, once being received on the mobile devices 300, is executed accordingly to reload the pre-
5 loaded messages on the SIM card. As a result of which, pre-defined configurations on the recipient SIM card can thus be modified via the RFM messages.

In one embodiment, the back-end host server 100 further includes a set of libraries, in which data management formats of each type of SIM Card available in the
10 art are maintained. Accordingly, the back-end host server 100 is capable of formatting the encrypted RFM messages so as to ensure that these messages are readable by the recipient SIM card of various types.

The OTA gateway 200 receives the RFM messages from the back-end host
15 server 100 through a secure gateway API of the OTA gateway 200. The gateway API directs the RFM messages so that they are transmitted to its recipient mobile devices 300. In one embodiment, the OTA gateway 200 is further adapted to transform the RFM messages into the SMS or USSD code format before transmitting them. These transformed RFM messages, which can be in the form of SMS or USSD code, are sent
20 to a Short Message Service Centre (SMSC) of the carrier. The SMSC then broadcast these messages to the recipient mobile devices 400 in the field.

Upon receipt of the RFM messages, the respective SIM card extracts the RFM command(s) contained therein. The extracted RFM command(s) executes Elementary File (EF) management commands of SIMToolkit (STK) on the SIM card. The Elementary File (EF) management commands include commands, such as, for example, SELECT, UPDATE RECORD, DEACTIVATE FILE, etc, which are configured to update the previously stored SIM messages accordingly. These commands are well known under the STK standard, and therefore no further detail and elaboration is provided herein. In another embodiment, the commands may be other proprietary commands that work only on devices from specific maker.

Accordingly, the back-end host server 100 is able to initiate an alert on SIM-based mobile device by re-configuring or overwriting the alert to replace the default messages embedded on the SIM of the mobile devices 300 at will. It is possible that the back-end host server 100 transmit the RFM messages to only a specific group device. It also allows the changes to be triggered at a pre-configured timing, such as hourly, daily, or whenever the device is switch on. It allows dynamic configurable text to be displayed at will on the user's devices through the SIM card.

In another embodiment, it is preferred that the SIM card is Alert Message Box Enabled. The Alert Message Box is a standard feature that can be triggered on and off. Once it is turned on, it allows text to be displayed as an alert on an alert box, not as a text message like SMS. Once displayed on the mobile device as an alert, there is

no option for the mobile devices' users to ignore the alert. Whether or not the alert is being read, users must acknowledge the alert to resume the functionalities of the mobile device. For example, a soft button labeled "OK" can be provided for the acknowledgement.

5

FIG. 2 exemplifies a screen shot from a mobile device as one embodiment. The screen shot shows a pop up window displaying "System Enabled" as an alert message when the phone is turned on and log-on into the mobile network. The alert message is preset on the SIM card to show that the alert message box is enabled.

10

FIG. 3 exemplifies a screen shot of the graphical user interface (GUI) of another embodiment. The screen shot is taken from the back-end host server 100 where the administrator may initiate to reconfigure the default message(s). The screen shot comprises a field for entering mobile phone(s), a selectable option to define what type of message to be sent from the back-end host server, and a text field for inputting the messages therein. The field for entering mobile phone may allow one or more mobile number to be entered. In another embodiment, it may provide a selectable option that leads to a database for selecting a bulk number mobile numbers with options to filter the phone numbers.

15
20

The administrator may also select from the selectable option whether a RFM message or a text message is to be sent. When a read text is elected, the administrator

may input the actual command into the SMS text field in order to reconfigure the default message stored on the SIM card, and the command are in human readable form. The command is executable by the mobile device to effect the changes on the SIM card. When a RFM message is selected, the command for reconfigure the SIM
5 card will appear in a machine readable form, which is encrypted, as shown in FIG. 3.

FIG. 4 exemplifies another screen shot on a mobile device in another embodiment. The message is shown as a pop up window at a prescribed time on the
10 mobile device. The prescribed time may be immediately after the device received the secured message from the back-end server 100, or a specific later time of desire. For example, the administrator of the back-end server 100 may set the SIM card to shows the message “Happy New Year!!” on a specific time and date, such as 00:00hr on 1 Jan 2013. In the FIG. 4, the pop up window displays “Happy New Year!!” with a
15 sender’s name appears on top at 00:00hr on 1 Jan 2013 as set by administrator. The mobile device user is required to press the button “OK” to close the message.

The secured message was send from the back-end server 100 to reconfigure the default message stored on the SIM card over the mobile communication traffic,
20 however, the message is displayed as a SIM-based alert without requiring any real time mobile communication traffic as such.

In another embodiment, it is also possible for the administrator to set the prescribed time to display on a specific operating state of the mobile device, such as next reboot, instead of a specific timing, or the like.

5 In another embodiment, the message to be displayed as the SIM-based alert may comprise hyperlink for lengthy message. The hyperlink is selectable by the mobile device user, which will lead the user to the actual content of the message to be displayed. The hyperlink may be a web page address that, once selected, the mobile device executes a default browser to display the web page.

10

As will be readily apparent to those skilled in the art, the present invention may easily be produced in other specific forms without departing from its essential characteristics. The present embodiments is, therefore, to be considered as merely illustrative and not restrictive, the scope of the invention being indicated by the claims
15 rather than the foregoing description, and all changes which come within therefore intended to be embraced therein.

CLAIMS

1. A system (10) for remote configuring or re-configuring pre-loaded SIM Card messages/texts of a SIM card residing on a communication device (300), comprising:

5 a back-end host server (100) connected to at least one carrier's network, wherein the carrier's network communicates the back-end host server with at least one SIM Card that is associated with the carrier's network; and

an Over-The-Air (OTA) gateway (200) adapted to direct management commands received from the back-end host server to its actual recipient SIM card.

10

2. A system (10) as claimed in Claim 1, wherein the back-end host server (100) includes at least one user interface device adapted to allow users to generate and to forward Remote File Management messages comprising configurations and/or re-configurations to the SIM card.

15

3. A system (10) as claimed in Claim 1, wherein the back-end host server (100) includes SIM card database for storing identification details of each SIM card that associated with the carrier's network.

20

4. A system (10) as claimed in Claim 1, wherein the back-end host server (100) includes a set of libraries, in which data management formats of each type of SIM Card types available in the art are maintained for formatting the encrypted Remote

File Management messages so that these management commands are readable by the recipient SIM card.

5. A system (10) as claimed in Claim 1, wherein the OTA gateway (300) is
5 further adapted to transform the Remote Management messages into either SMS or
USSD code format before transmitting them into its recipient SIM card.

6. A system (10) as claimed in Claim 1, wherein the OTA gateway (300) further
includes a Short Message Service Centre (SMSC) for receiving and transmitting the
10 Remote Management messages in SMS or USSD code format to its recipient SIM
card.